InfraGard
Maine

InfraGard Maine at MTUG

Laws, Wars, and Threat Hunting

Frank Appunn

Agenda

- Welcome
- Laws
- Wars
- Threat Hunting
- Q&A
- Close & Contact Information

InfraGard Maine

Welcome

InfraGard Maine

InfraGard is a partnership between the Federal Bureau of Investigation (FBI) and members of the private sector for the protection of U.S. Critical Infrastructure. Through seamless collaboration, InfraGard connects owners and operators within critical infrastructure to the FBI, to provide education, information sharing, networking, and workshops on emerging technologies and threats.

InfraGard's membership includes: business executives, entrepreneurs, lawyers, security personnel, military and government officials, IT professionals, academia and state and local law enforcement—all dedicated to contributing industry-specific insight and advancing national security.

Laws and Regulations

- **Cyber Incident Reporting for Critical Infrastructure Act of 2022 (Strengthening American Cybersecurity Act 2022)**
  - Report 72 hours after discovery, ransomware payment in 24 hours
  - Failure to report to CISA can be a DOJ Subpoena
  - Breadth can grow
- Implications
  - Must show infrastructure and capability
  - CISA taskforce and repository for use by DOJ and FBI
  - Rise of the CISO
  - Tough choices for reporting …

InfraGard Maine

Laws and Regulations

- Privacy
  - GDPR
  - California: CCPA and CPRA, plus Utah, Colorado, Virginia
  - Nebraska, Massachusetts, Maine, in process: OK and MD
  - In Committee NE, LA, AK, KY, NC, OH, PA, NJ, NY, CT, RI, MA, VT
  - Hotbed of change
  - Apply to all organizations in all states
  - Implications: What do you do?
  - https://iapp.org/resources/

InfraGard Maine

Laws and Regulations

- PCI DSS 4 of March 2022
  - Effective dates up to March 2025, from Version 3.2.1 retirement March 2024

- Roles & Responsibilities - everywhere
- Technical: Limit display of PAN and remote access, disk encryption on portable devices
- Phishing protection for users
- Monitor all web applications
- Access management: People, services, applications
- Identity Password strength & MFA
- Audit automation
- Monitor controls & report failures:

  vulnerability, IDS & IPS ,tamper detection
- Targeted risk assessments

  annual, but service providers 6 months
- Logical separation from clients
- Report test & incidents with addresses

  Include suspected incidents

  PAN location detail

InfraGard Maine

Wars – what can we learn and assume

- Ukraine
  - Fake everything
  - Leveraged widely
  - Starlink
  - Anonymous
- Russia
  - Power and ransomware
  - REvil arrest, really? Continuous evolution
  - Evolution beyond ransomware
    1) Shock and awe
    2) Automation to smaller sites
    3) Move to revenge and hate, not only money?

InfraGard Maine

Silent Wars

- Iran – destructive
- North Korea fishing, financial ransomware,
  - Indirect because of financial services blocks
- Taiwan
  - Chips: not easy to change
  - Collaboration
  - Weakness in US

InfraGard Maine

Is there room for Supply chain?

- What is it?
  - Keeping your supply chain functional and integrated
  - Assessing cyber and other risks for suppliers and customers
  - Assessing risk from communicating:
    - Information
    - Updates to programs
    - Data sharing
    - AI manipulation

SolarWinds
FireEye – Mandiant
LAPSUS$

Identity
Access Control
Cloud links
Resilience
Threat Intelligence
Anticipate issues

- NIST Cybersecurity Framework and controls SP 800-53r5 & 53A

Threat Hunting

- What are the top threats?
- Where do you pull from?
  - Industry
  - MITRE
  - NIST
- Does Hunting help you tackle the threat?
- What about the Risk?

InfraGard Maine

Threat Hunting Best Practices

- Think like an attacker.
- Head to the source.
- Don't forget the basics.
- Establish complete network visibility.
- Make security—not attacks—an inside job.
- Practice constant vigilance.
- Network visibility suite.
- Data logs – Pay Attention

InfraGard Maine

InfraGard Maine

Questions?

InfraGard Maine

Contact information

Frank Appunn frank@appunn.net
InfraGard https://www.infragard.org